PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :		(11) International Publication Number:	WO 92/04671
G06F 1/00, G07F 7/10	A1	(43) International Publication Date:	19 March 1992 (19.03.92)

(21) International Application Number: PCT/US91/06002

(22) International Filing Date: 22 August 1991 (22.08.91)

(30) Priority data:
574,640 29 August 1990 (29.08.90) US

(71) Applicant: HUGHES AIRCRAFT COMPANY [US/US]; 7200 Hughes Terrace, Los Angeles, CA 90045-0066 (US).

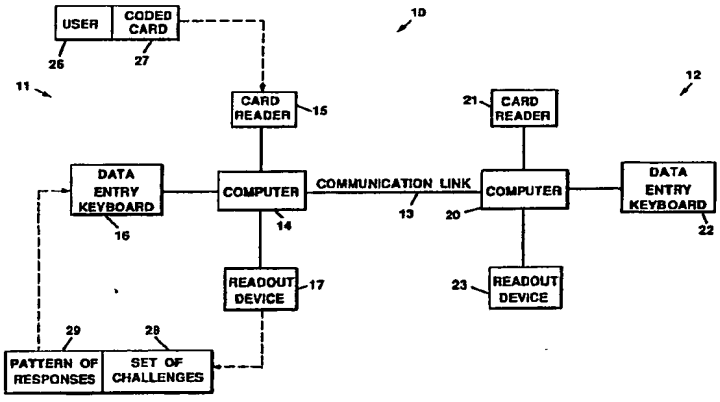
(72) Inventor: KUNG, Kenneth, C. ; 19029 Vickie Avenue, Cerritos, CA 90701 (US).

(74) Agents: DAUBENSPECK, William, C. et al.; Hughes Aircraft Company, Post Office Box 45066, Bldg. C1, M/S A126, Los Angeles, CA 90045-0066 (US).

(81) Designated States: AT (European patent), BE (European patent), CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, LU (European patent), NL (European patent), NO, SE (European patent).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: DISTRIBUTED USER AUTHENTICATION PROTOCOL



(57) Abstract

A distributed authentication system that prevents unauthorized access to any computer system (10) in a distributed environment. Authentication using the present invention involves three distinct phases. In the first phase, user passwords are generated by the computer system (10) and encrypted on a coded card (27) together with a message authentication code to prevent alterations prior to any access attempts. These are complex and impersonal enough not to be easily guessed. This coded card (27) must be used whenever requesting access to the system (10). Second, in addition to supplying a password, the user is required to correctly respond to a set of randomly selected authentication challenges (28) when requesting access. The correct responses (29) may vary between the right response, a wrong response or no response depending on some predetermined variable, e.g., the day of the week or hour of the day. The dual randomness thus introduced significantly reduces the usefulness of observed logon information. Third, at random times during the session, the user is required again to respond to selected authentication challenges (28). This detects piggybacking attempts. Since authentication depends on the correctness of the entire set of responses (29) rather than on the response to a single question, the present invention provides a significant increase in the probability of detecting and preventing unauthorized computer access.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland			SN	Senegal
CI	Côte d'Ivoire	KR	Republic of Korea	SU+	Soviet Union
CM	Cameroon	LI	Liechtenstein	TD	Chad
CS	Czechoslovakia	LK	Sri Lanka	TG	Togo
DE*	Germany	LU	Luxembourg	US	United States of America
DK	Denmark	MC	Monaco		

+ Any designation of "SU" has effect in the Russian Federation. It is not yet known whether any such designation has effect in other States of the former Soviet Union.

DISTRIBUTED USER AUTHENTICATION PROTOCOL

BACKGROUND

The present invention relates to authorized user recognition in a distributed computer system and, more particularly, to the use of computer passwords and other computer user recognition protocols.

There is an inherent danger in any computer system where intruders, using normal channels, may access sensitive or classified information for malicious purposes. Unauthorized users can cause many problems for computer systems. They may modify software to cause unwanted events to occur or to benefit themselves. They may access private or classified data, copy proprietary software, etc. While doing all this, they can seriously impact all computer-based operations when their use of computer resources causes deterioration of response times or denial of service for legitimate users. Such access can be accomplished in a number of ways, e.g., the user claims to be someone else, the user diverts the access path to another computer system, the user accesses the system before a legitimate user logs off, and the like.

Access can be gained by persons who observe a legitimate logon session within an open communication network and later masquerade as that legitimate user by using the information seen. Simple, user-selected and often personally related passwords can be "guessed" by intruders or programs written by them. Legitimate sessions may be recorded from the communication network for later playback or an intruder may "piggyback" a legitimate session by using the system before the user has logged out.

To guard against such attacks, the system must protect itself by authenticating its users. Passwords and authentication responses can also be obtained by collusion or

surreptitious means. These are outside the scope of the authentication process. The present invention's effectiveness against that type of an attack is limited to the case where only an incomplete set of responses was obtained and thus tests are failed.

The use of passwords to authenticate users is the most prevalent means of controlling access currently in use. In many cases, the users select their own passwords or continue to use the group password. Studies have shown that most users select passwords that are easy to remember, generally personal in nature and seldom change them. Under these circumstances, they are easy to guess either by a motivated individual or a simple program using a random word generation technique.

Some systems may use an authentication means such as requesting the user to supply a sequence of names, etc. in conjunction with a password. This makes entry more difficult but is still vulnerable if the logon procedure is observed and the response identified or the expected response is easy to guess. Neither the authentication mechanism nor the password scheme provide the protection against piggybacking, the use of a system before a legitimate user logs off, imbedded in the present invention.

Accordingly, there is a need for a foolproof means of recognizing and authenticating an authorized user in a computer system.

SUMMARY OF THE INVENTION

In accordance with these and other objectives and features of the present invention, there is provided a distributed authentication system that prevents unauthorized access to any computer system in a distributed environment. Restriction of access is a major step in preventing destructive modification of software or data, improper release of sensitive/classified information, and misuse of computer system resources. One unique feature of the present invention is the use of multiple, randomly selected authentication or challenge mechanisms and a wide variety of correct answers. "Correct" answers may include right, wrong, or no responses. Since authentication depends on the correctness of the entire set of responses rather than on the response to a single question, the present invention provides a significant increase in the probability of detecting and preventing unauthorized computer access.

Authentication using the present invention involves three distinct phases. In the first phase, user passwords are generated by the computer system and encrypted on a coded card together with a message authentication code to prevent alterations prior to any access attempts. These are complex and impersonal enough not to be easily guessed. This coded card must be used whenever requesting access to the system. Second, in addition to supplying a password, the user is required to correctly respond to a set of randomly selected authentication challenges when requesting access. The

correct responses may vary between the right response, a wrong response or no response depending on some predetermined variable, e.g., the day of the week or hour of the day. The dual randomness thus introduced significantly reduces the usefulness of observed logon information. Third, at random times during the session, the user is required again to respond to selected authentication challenges. This detects piggybacking attempts.

The authentication invention described herein performs these functions in a distributed as well as a centralized environment. It employs pairs of authentication boxes, coded cards, passwords and a selection of challenges. Distributing responsibility for authentication between the user node and the computer system permits a user to access different computer systems from a single user node. The only restriction is that the user must possess one or more coded cards generated by the computer(s) to be accessed. The challenges used are selected at random for each authentication session. Responses to the challenges can also be varied. At one time, a true response may be expected. At another, no answer or a false answer may be the correct response. The pattern of these responses can be varied by basing their selection on a parameter such as day of the week, if desired. Access is granted based on reception of correct responses to the entire set of challenges. Users are required to remember their password and the valid pattern of response to gain access to the system. Care must be taken that the response patterns are easy enough to remember so that users will not be tempted to record them in an unsafe location.

BRIEF DESCRIPTION OF THE DRAWINGS

The various features and advantages of the present invention may be more readily understood with reference to the following detailed description taken in conjunction with the accompanying drawings, wherein like reference numerals designate like structural elements, and in which:

FIG. 1 is a block diagram of a simplified computer system employing the principles of the present invention; and

FIG. 2 is a diagram of a second embodiment of the distributed computer system employing the principles of the present invention.

DETAILED DESCRIPTION

Referring to the drawings, FIG. 1 is a block diagram of a simplified exemplary arrangement of physically separated computer installations electrically interconnected to form a distributed computer system 10. The distributed computer system 10 comprises a first terminal 11 and a second terminal 12 interconnected by a communication link 13.

The first and second terminals 11, 12 are physically separated, and may be on different continents, or in different rooms of the same building. The communication link 13 may comprise wires or coaxial cables, a microwave link, or a path by way of a communication satellite or communication network. The first terminal 11 comprises a computer 14 connected to a card reader 15, a data entry keyboard 16 and a readout device 17. Similarly, the second terminal 12 comprises a computer 20 connected to a card reader 21, a data entry keyboard 22 and a readout device 23. The computers 14, 20 may be any conventional unit such as an IBM, MacIntosh or any mainframe. The card readers 15, 21 may be a box with a card slot and a magnetic reader inside or an optical reader for reading a bar code printed on the card, or any other suitable card reading arrangement. The data entry keyboard 16, 22 may be a keypad or a conventional computer keyboard, or the like. The readout device 17, 23 may be a liquid crystal display, a cathode ray tube monitor or a hard copy printer.

In operation, a user 26 approaches the first terminal 11 and presents a coded card 27 to the card reader 15. The card reader 15 reads the code on the card 27. The computer 14 verifies the authenticity of the card 27 by checking the code against authentication data stored in card 27. If authentic, the computer 14 requests a password by way of the readout device 17. The user 26 enters the password by way of the data entry keyboard 16. The computer 14 compares the password with a password stored on the coded card 27. If not authentic, communications are terminated.

If the password is authentic, the computer 14 at the first terminal 11 initiates communications with the computer 20 at the second terminal 12. After a handshaking and authentication protocol has been completed, the computers 14, 20 have authenticated each other, and a trusted path now exists between them.

The computer 20 at the second terminal 12 now proceeds to present a set of challenges 28 via the readout device 17 at the first terminal 11. The user 26 responds to the challenges 28 via the data entry keyboard 16 at the first terminal 11. The computer 20 at the second terminal 12 compares the pattern of responses 29 given with a stored pattern of responses 29 agreed upon ahead of time. It is a feature of the present invention that the correct pattern of responses 29 includes some "incorrect answers" given on purpose. For a set of five challenges 28, it may be agreed upon ahead of time that three of the responses 29 will be correct, and that two of the responses 29 will be incorrect. The set of challenges 28 and the pattern of responses 29 are deliberately made easy to avoid the need for writing them down as a memory aid. The key is in the agreed upon pattern of responses 29. Seven out of ten correct - any seven - or a particular seven. The pattern of responses 29 can vary from day-to-day or from morning to afternoon. The pattern of responses 29 can be different for each user. When there

are two or more distant terminals to be accessed, the recognition pattern of responses 29 can be different as one user accesses different terminals.

The present invention prevents unauthorized access to any computer system in a distributed environment. Restriction of access is a major step in preventing destructive modification of software or data, improper release of sensitive/classified information, and misuse of computer system resources. One unique feature of the present invention is the use of multiple, randomly selected authentication mechanisms and a wide variety of correct answers. "Correct" answers may include right, wrong, or no responses. Since authentication depends on the correctness of the entire set of responses rather than on the response to a single question, the present invention provides a significant increase in the probability of detecting and preventing unauthorized computer access.

Authentication using the present invention involves three distinct phases. In the first phase, user passwords are generated by the computer system and encrypted on a coded card together with a message authentication code to prevent alterations prior to any access attempts. These are complex and impersonal enough not to be easily guessed. This coded card must be used whenever requesting access to the system. Second, in addition to supplying a password, the user is required to correctly respond to a set of randomly selected authentication challenges when requesting access. The correct responses may vary between the right response, a wrong response or no response depending on some predetermined variable, e.g., the day of the week or hour of the day. The dual randomness thus introduced significantly reduces the usefulness of observed logon information. Third, at random times during the session, the user is required again to respond to selected authentication challenges. This detects piggybacking attempts.

The authentication invention described herein performs these functions in a distributed as well as a centralized environment. It employs pairs of authentication boxes, coded cards,passwords and a selection of challenges. Distributing responsibility for authentication between the user node and the computer system permits a user to access different computer systems from a single user node. The only restriction is that the user must possess one or more coded cards generated by the computer(s) to be accessed. The challenges used are selected at random for each authentication session. Responses to the challenges can also be varied. At one time, a true response may be expected. At another, no answer or a false answer may be the correct response. The pattern of these responses can be varied by basing their selection on a parameter such as day of the week, if desired. Access is granted based on reception of correct responses to the entire set of challenges. Users are required to remember their password and the valid pattern of response to gain access to the system. Care must be taken that

the response patterns are easy enough to remember so that users will not be tempted to record them in an unsafe location.

FIG. 2 illustrates a second example of an operational arrangement. In this system, the user can access any computer in a distributed system from a single node provided that he possesses a coded card containing a password generated by that computer.

FIG. 2 is a block diagram of another embodiment of a distributed computer system 30 having five nodes 31, 32, 33, 34, 35. Each node 31, 32, 33, 34, 35 is comprised of a computer system 36 and an authentication box 37. In the present example, the authentication box 37 at the fifth node 35 has communication links 38 to the authentication boxes 37 at the first, second and third nodes 31, 32, 33. Similarly, the authentication box 37 at the fourth node 34 has communication links 40 to the authentication boxes 37 at the first, second and third nodes 31, 32, 33. A first user 41 is located at the fifth node 35, and a second user 42 is located at the fourth node 34. Since authentication boxes 37 are colocated with their respective computer system 36, the path between each box 37 and its computer system 36 is considered to be trusted.

The following describes the operation. Protection against fraudulent responses to messages sent over the communication links 38, 40 is provided through the use of time stamps and sequence numbers. An intruder cannot decrypt a message in time to generate a response within the acceptable time window or determine the proper sequence number for the set that applies.

Prior to the start of communications, the first node 31 must: (a) generate two asymmetric keys: AKc which is stored on the user's card and AKx which is stored in the first node 31 associated with the user's password file, and (b) generate a card to be carried by the first user 41 using a private key (PKcard). This card contains the user name, encrypted password, AKc, Message Authentication Code (MAC).

To initiate a session, the first user 41 presents a card to the authentication box 37 at fifth node 35. The fifth node 35 authenticates the card by checking the MAC. If authentic, the fifth node 35 authenticates the first user 41 by requesting the password, encrypting it and comparing it with the password stored on the card. If not authentic, communications are terminated. If authentic, the fifth node 35 sends a message to the authentication box 37 at the first node 31 encrypted with the public code of the first node 31 and containing the certificate of the fifth node 35, a date/time stamp, a sequence number, a random number generated by the fifth node 35 and a MAC. If not authentic, communications are terminated.

The first node 31 decrypts the message and verifies that the fifth node 35 is not on the list of compromised authentication boxes 37 furnished by the an authority desig-

nated as the Key Management Center. If the fifth node 35 is on this list, the first node 31 considers the card for the first user 41 also to be compromised and terminates communications. If the fifth node 35 is not on this list, the first node 31 checks the time stamp to determine if it is within a predetermined window. If not, the message is considered invalid and communications are terminated. If valid, the first node 31 checks the sequence number to verify that it is in consecutive order for the fifth node 35. If not, the message is considered invalid and communications are terminated. If valid, the first node 31 sends a message to the fifth node 35 encrypted with the public key of the fifth node 35 and containing the certificate of the first node 31, a date/time stamp, a sequence number, the random number generated by the fifth node 35 and a MAC.

The fifth node 35 decrypts the message and performs the same time stamp and sequence number tests as discussed in the last paragraph. If not passed, communications are terminated. If passed, the fifth node 35 generates a traffic encryption key TEKab using both certificates and the random number. At this point, the fifth node 35 and the first node 31 have authenticated each other and a trusted path now exists between them.

Using the traffic encryption key TEKab, the first node 31 sends a message to the fifth node 35 containing a request for the password of the first user 41 and a MAC. The fifth node 35 requests the password of the first user 41. The first user 41 enters a clear test password. The fifth node 35 encrypts the password then using TEKab to send it to the first node 31 with a MAC. The first node 31 compares the encrypted password with the one stored in the first node 31. Only three attempts to enter a password are allowed. If three failures occur, the session is terminated.

If the password is accepted, the first node 31 downloads challenges from its authentication box 37 to the fifth node 35. The authentication box 37 at the first node 31 selects the challenges randomly and sends a message to the fifth node 35 encrypted with TEKab containing the challenge/response phrases and a MAC. The preceding step is repeated a random number of times with different authentication challenges. Only one opportunity is allowed for response to each challenge. The fifth node 35 sends a message encrypted with TEKab containing the sequence of passed/failed challenges of the first user 41 and a MAC. If first user 41 has failed to supply the proper sequence of passed/failed challenges, the session is terminated. The first node 31 repeats authentication requests at intervals during the session to provide continuous authentication. Whenever the session terminates, the fifth node 35 will destroy all downloaded information and notify the first node 31 when completed using TEK for encryption.

Thus there has been described a new and improved method for recognizing an authorized user in a computer system. It is to be understood that the above-described embodiments are merely illustrative of some of the many specific embodiments which represent applications of the principles of the present invention. Clearly, numerous and other arrangements can be readily devised by those skilled in the art without departing from the scope of the invention.

What is claimed is:

1. A user authentication arrangement for use with a computer network (10) having physically separated nodes, said arrangement characterized by:

first and second nodes (11, 12) each including a computer (14, 20), a readout device (17, 23) and a keyboard (16, 22), and at least one of said nodes (11) having a card reader (15);

a communication link (13) operatively interconnecting said nodes (11, 12); and

a coded card (27) adapted to be read by the card reader (15) and having a coded message stored thereon that is compared with a correct message stored in a selected node (11), whereupon, if the coded message agrees with the correct message, a set of challenges (28) is displayed at the readout device (17) and responses are entered by the user on the keyboard (16), and the pattern of responses entered by the user, including correct and incorrect responses, is compared with the preselected agreed upon pattern of responses (29) to determine user access to the computer network (10).

2. A method for authenticating an authorized user for a computer network (10) having physically separated nodes (11, 12) that each comprise a computer (14, 20), characterized by the following steps:

inserting a coded card (27) in a card reader (15);

comparing the code contained on said card (27) with a correct code stored in the computer (14);

displaying a preselected set of challenges (28) to the user;

responding to the preselected set of challenges (28) with a pattern of responses including correct and incorrect responses and no responses, whereupon, the pattern of responses entered by the user, including correct and incorrect and no responses, is compared with the preselected pattern of responses (29) to determine user access to the computer network (10).

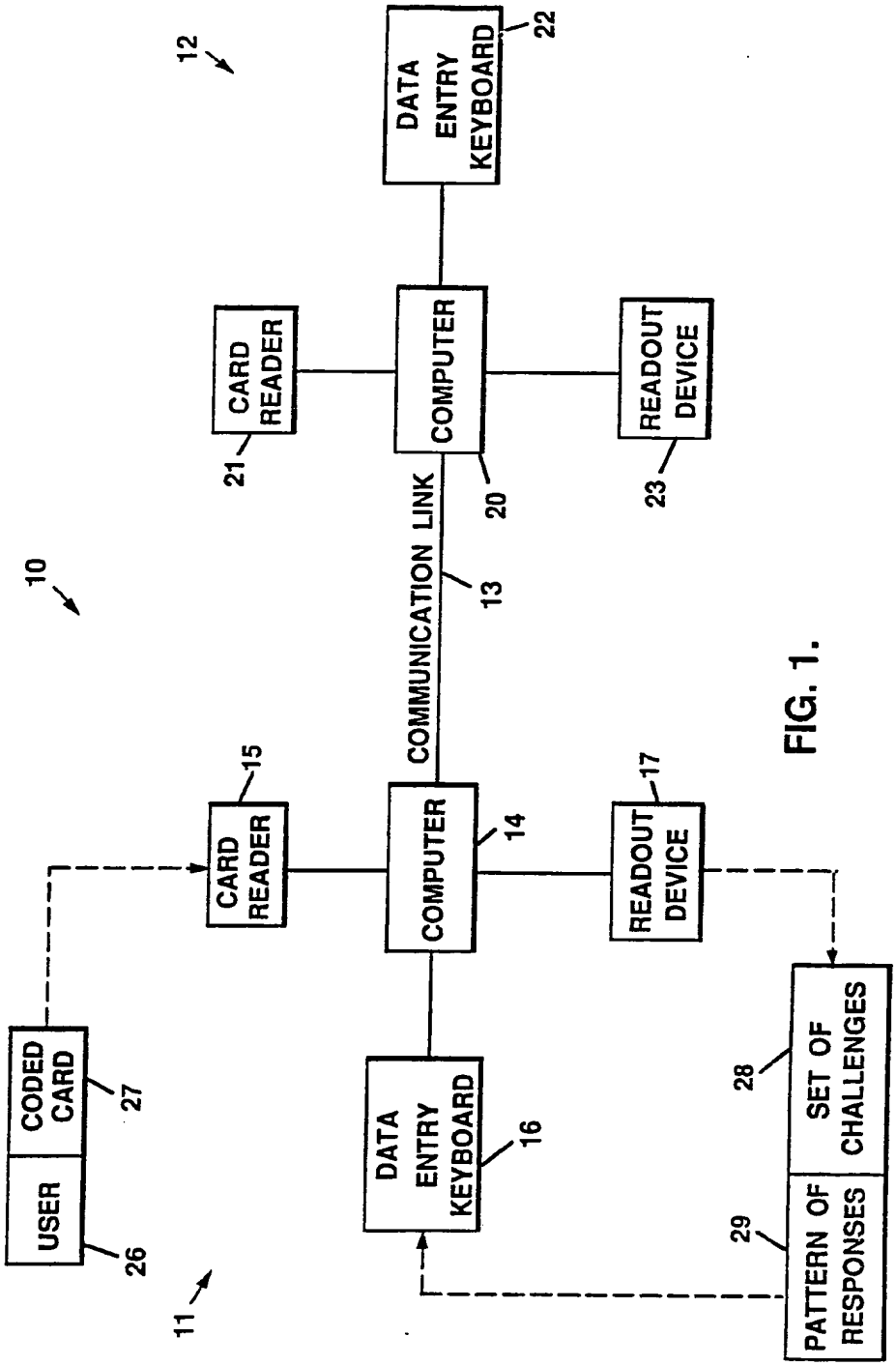

12
DATA ENTRY KEYBOARD
22
CARD READER
21
COMPUTER
20
READOUT DEVICE
23
COMMUNICATION LINK
13
10
15
CARD READER
COMPUTER
14
READOUT DEVICE
17
CODED CARD
27
USER
26
DATA ENTRY KEYBOARD
16
28
SET OF CHALLENGES
29
PATTERN OF RESPONSES
11

FIG. 1.

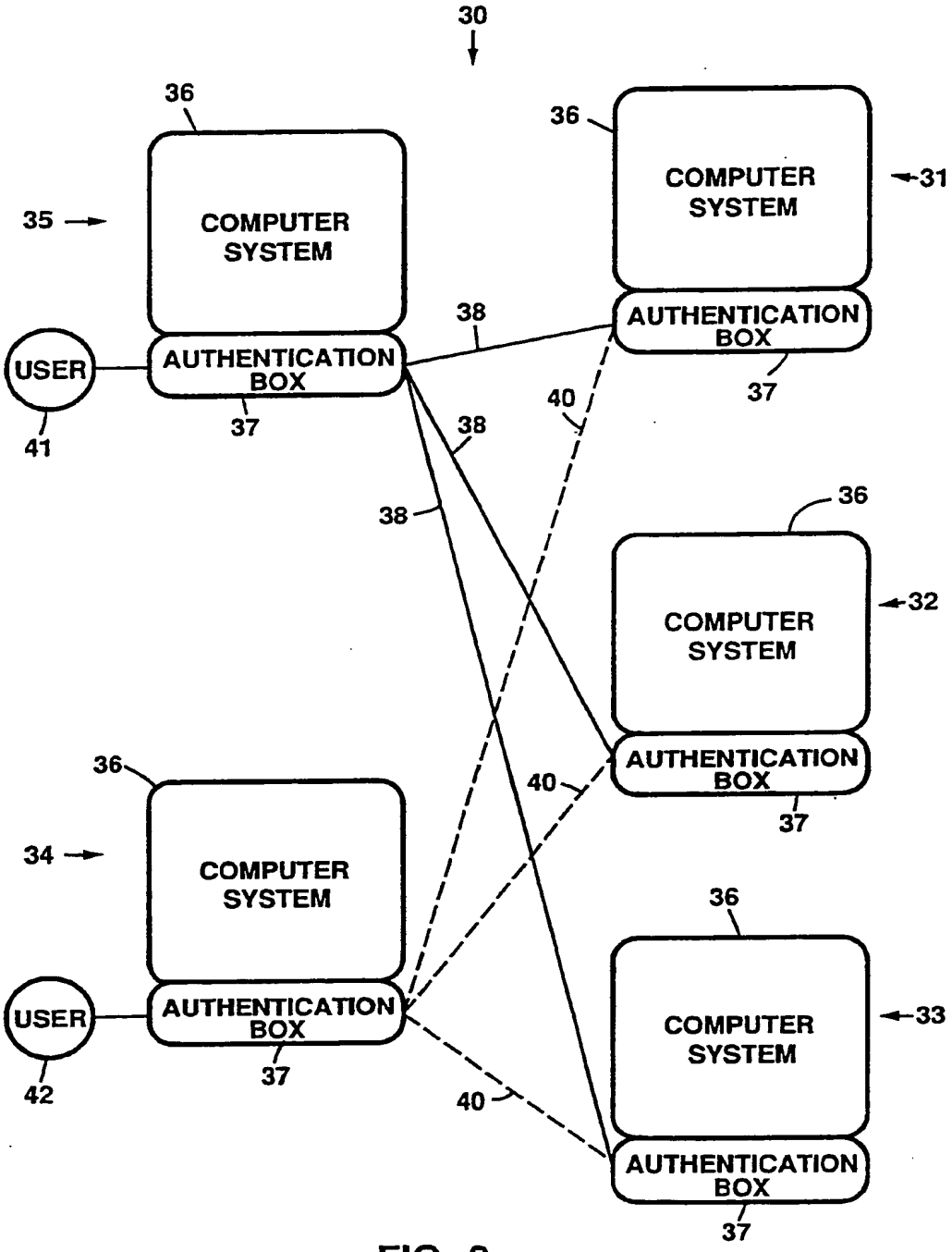

30
36
COMPUTER SYSTEM
35
31
AUTHENTICATION BOX
USER
38
37
41
40
32
34
33
42

FIG. 2.

INTERNATIONAL SEARCH REPORT

International Application No PCT/US 91/06002

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all)[6]

According to International Patent Classification (IPC) or to both National Classification and IPC

Int.Cl. 5 G06F1/00 ; G07F7/10

II. FIELDS SEARCHED

Minimum Documentation Searched[7]

Classification System	Classification Symbols
Int.Cl. 5	G06F ; G07F

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched[8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT[9]

Category [10]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No.[13]
Y	WO,A,8 807 240 (SIEMENS LTD.) 22 September 1988 see figures 2A,2B see page 6, line 18 - line 33 see page 11, line 13 - line 19	1,2
Y	FR,A,2 584 514 (CASIO COMPUTER CO. LTD.) 9 January 1987 see figures 1,5A-5D see page 2, line 8 - line 34 see page 3, line 3 - line 20	1,2

* Special categories of cited documents : [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
27 DECEMBER 1991	09.01.92
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	WEISS P.

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON INTERNATIONAL PATENT APPLICATION NO. US 91/06002

SA 52412

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

06/01/92

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO-A-8807240	22-09-88	AU-A- 1483788	10-10-88
FR-A-2584514	09-01-87	JP-A- 62009470	17-01-87
		DE-A,C 3622257	15-01-87
		US-A- 4801787	31-01-89

EPO FORM P0479

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82